A Strategic Framework for Addressing the most Tactical of Problems: It’s all about the Bad Guys

Russell E. Travers
Counselor, National Counterterrorism Center

This paper, written in August 2015, was selected as a Finalist in the 2015/2016 Galileo Awards Program. Galileo is an annual Intelligence-wide competition designed to encourage and recognize innovative workforce ideas that address current challenges and help share the future of U.S. Intelligence.

All statements of fact, opinion or analysis expressed are those of the author and do not reflect the official positions or views of the National Counterterrorism Center or any other U.S. Government (USG) agency. Nothing in the contents should be construed as implying USG or NCTC endorsement of the author’s views. This material has been reviewed to prevent the disclosure of classified information

Introduction

Strategic challenges posed by nation states and evolving geopolitical trends have been, and will be, with us forever. There have been some modifications in tradecraft and analytics, but the nature of the problem set hasn’t dictated any fundamental change in the way we do business. But another challenge has emerged and we haven’t adequately responded. Globalization has empowered individuals like never before. Terrorism, proliferation, transnational organized crime and financial fraud are certainly not new. But practitioners of those activities have been supercharged and it is imperative that we posture ourselves accordingly to mitigate the threat. The most tactical of problems – the actions of individual bad actors, can now have strategic effects, so we’ll need to improve our ability to discern who they are, and then catalogue their identifiers, what they are doing, how they are doing it, and with whom they are connected. And then we need to make sure that all elements of the Government with an appropriate interest can make use of the information. It requires a new way of doing government-wide business, patterned after lessons we have learned from our counter terrorism efforts. This article lays out a strategic framework for addressing the most tactical of issues, the challenges posed by transnational bad actors[1].

You might think that the Government maintains an integrated master data base of known and suspected bad guys, a list that integrates biographic and biometric information, along with a dossier of what they’ve done, so that if that if any of those individuals tries to commit visa fraud to enter the Country… or reach out to a known or suspected terrorist… or utilize our financial system… or visit sensitive facilities… or gain control of U.S. infrastructure…or conduct any other activity reasonably considered a security threat to the Country… that the Government would be well postured to collectively maintain situational awareness, understand the contours of the problem, share relevant information, properly watchlist them, and take any other appropriate action. You might think that. But you would be wrong.

[1] The central theme of this article is the need to leverage CT lessons learned and to integrate intelligence with other elements of state power to address the threat posed by transnational threat actors. In doing so, however, it is self–evident that the Intelligence Community will only operate in areas in which it has the legal authority to do so.

Giving Other Transnational Threat Actors the Focus They Deserve

Making the case for Bin Laden as a strategic actor is/was obvious. It should be apparent that an AQ Khan global proliferation network would be equally concerning. And when we talk about a trillion dollar TOC cesspool… or the prospect of a counter intelligence penetration of our Community… or cyber as the greatest transfer of wealth in human history, it should be self-evident why we need to do a far better Government-wide job of tracking the actors and associated networks.

While we have spent the last twelve years institutionalizing and improving such a system for terrorism, there is no integrated effort for any other category of nefarious actors. We have some databases that are shared to greater or lesser degrees. But there is no central and shared repository of such known and suspected transnational bad guys. To the extent Government entities submit names to various watchlists, it is done in an ad hoc manner. Tippers may be created, but there is little or no coordination between/among organizations, no sustained focus on quality control, no effort to enhance records to improve our knowledge about the individual or determine to whom he is connected, no focused deletion of outdated records, no integration of biographics and biometrics, and no institutionalized approach to automatically downgrading information necessary for screening. For all categories of nefarious actors other than terrorists, the business process and architectural "plumbing" across the Government look largely the way they did for terrorism before 9/11. It is the absolute antithesis of integration. And it needs to change.

A BRIEF REFRESHER: THE ART OF THE POSSIBLE AS REFLECTED IN OUR APPROACH TO COUNTERTERRORISM

9/11 is often portrayed as a failure of information sharing. And it was, in part. But the more fundamental problem was architectural. It was a lack of government-wide integration. Parts of the government knew about Khalid al Midhar and Nawaf al Hazmi - the two hijackers who had been associated with the East Africa bombings, were known to the CIA, and yet were able to subsequently get visas and freely move in and out of the Country. Other parts of the government, the FBI and State Department in particular, had no idea – until it was too late, who they were or why they were important. Why? Because before 9/11 we had multiple lists of known and suspected terrorists and we had 13 national watch lists. Unfortunately none of those lists were either interoperable, or broadly accessible. As a result, 9/11 plotters were able to acquire almost 2 dozen visas and successfully crossed our borders almost 3 dozen times.

The causes of the failure were quickly diagnosed and the fixes were straightforward. We created the National Counterterrorism Center (NCTC) and, among other things, charged it with maintaining the single authoritative U.S Government "shared knowledge base" of known or suspected terrorists. And we created the Terrorist Screening Center (TSC) to serve as the interface with all organizations that have a screening responsibility. With the "middleware" in place, we enabled a logical business process: all collectors reviewed their own intelligence reporting and provided appropriate details to the NCTC which consolidated, cross referenced, quality controlled and supplemented the information in the classified TIDE (Terrorist Identities Datamart Environment) database which serves as the Country's master repository of terrorist identities' information. NCTC, in turn, provides a sensitive but unclassified extract to the TSC which maintains the master unclassified watchlist, the Terrorist Screening Database (TSDB). And TSC provides the screening Community with the information needed to support their respective missions, based on timelines, level of granularity, and specificity required by particular screeners.

The Ultimate Example of Integration

Consider the power of our terrorism watchlisting enterprise. If CIA collects terrorist identities information overseas, an extract is available to support a CBP officer who stops that individual on the Canadian border. If DIA collects information in Afghanistan, knowledge about that individual is available to support a police officer who encounters that person during a traffic stop in Baltimore. If FBI collects information domestically, it can support a No Fly decision should that individual try to board a plane from Frankfurt to the United States. Or if NSA collects information in Central Asia it is available to support a consular officer who may encounter that same individual in Beijing seeking a U.S. visa. In other words if the U.S. Government has knowledge about a known or suspected terrorist, any other part of the Government that may require such knowledge to do its job has the relevant information. What better example exists of integration? And it only works because we start with a single repository of known and suspected terrorists that supports others in the Government who have a legitimate need for such information.

The Challenge of Identities' Analysis

None of this is easy. Positively identifying a person is a difficult analytic problem. And using a names-based system is particularly challenging. Recall the 9/11 Commission finding that the hijackers used 362 name variants. Or… the news reports from several years ago that noted there were in excess of 100 accepted spellings of former Libyan dictator Mummar Qadafi's name. Naming conventions, honorifics, the lack of a standard Romanization regime to transliterate Arabic to English, kunyas (nicknames), as well as the use of false identities and stolen documentation, are standard fare for identities analysts. We obviously recognized the limitations of a names based system, but it was all we had after 9/11 - we simply didn't have biometrics on most known or suspected terrorists. Nevertheless we got pretty good with what we had, continually correcting deficiencies as we got increasingly sophisticated in our approach.

And over time we got better. An Executive Order in 2008 initiated a concerted Government-wide effort to utilize biometrics to enhance our identities analysis. It was complicated because numerous repositories existed and sharing arrangements were cumbersome. But it was a start. The science of facial recognition improved, and as the Defense Department, in particular, collected fingerprints in Iraq and Afghanistan our ability to do comprehensive identities analysis improved markedly.

In addition, a State Department detailee to NCTC began experimenting with, and advocating for, a more comprehensive use of available data to bolster our screening capabilities. Known as the Kingfisher program, the effort sought to more fully utilize visa applicant information to determine potential terrorist linkages. Over time the process has grown increasingly sophisticated. Automation allows electronic visa applications to be compared, in near real time, against highly classified intelligence community holdings, thus enhancing the rigor of the screening. And equally important, this process has enabled "continuous vetting" which responds to an inherent limitation of intelligence; our identities analysis had traditionally been valid for a given point in time, and if additional information came in subsequent to that analysis, the screener would have no way of getting the benefit of that additional information. Now, with continuous vetting, if derogatory information becomes available subsequent to an individual being given a visa, the government will be apprised of that fact and can take appropriate steps.

Screening:
A Hard Problem – with no Panacea

Even with the significant investments we have made in terrorist identities and screening, the problem is daunting. The Syrian refugee challenge is illustrative. Let's assume that 99.99% of all refugees are simply innocent victims and perhaps 1/100th of one percent are ISIS members or individuals with ISIS sympathies. If we're talking about a refugee population of roughly 4 million people, that would equate to 400 individuals of concern. Could we detect them? It would depend entirely on the extent of our knowledge base about such individuals; unfortunately those that overstate either the extent of the actual threat, or our ability to detect a small number of nefarious actors in a sea of human suffering, undermine the Country's ability to have an informed discussion about risk. The lesson is simple: there is no question that we can do far better than we are now in screening for other categories of bad guys, but the fact remains that this is art, not science, and we are dealing with significant unknowns and intelligence gaps. Expectations need to be managed.

A STRATEGIC ROADMAP FOR ADDRESSING OTHER TACTICAL, IDENTITIES-RELATED THREATS

The Government could learn many valuable lessons from our counterterrorism experience. The policies, procedures, business processes and technical tools developed to help catalogue known and suspected terrorists could be used for analogous purposes against other categories of nefarious actors within the IC's authority to pursue. The strategic framework could be applied in the following four steps:

Step 1: Start by Pinning the Rose:

We have to get past the intellectual log jam of believing that this kind of work can be done in an ad hoc decentralized fashion; instead, there needs to be responsibility and accountability, along with the necessary resources, directed to an organization whose mission it is to keep book on the particular category of bad guys. The relevant analysts will be responsible for culling through intelligence and law enforcement traffic and creating a "TIDE-like" data base of those bad actors in which we have a government wide interest: for instance, categories of transnational criminal actors, individuals aiding and abetting cyber-criminal activities, proliferators, and individuals in which there will be counter intelligence and economic espionage interest. The responsible organizations would maintain appropriately classified data bases, which, much like TIDE for terrorists, would serve as the Government's shared knowledge base, aggregating what we need to know about the individual - including biographic and biometric identifiers, along with whatever additional information is needed to highlight the nature of their nefarious activity, and links to other individuals. A decade plus of doing this work in the realm of counterterrorism makes one lesson unmistakably clear: any chance of success requires a critical mass of well-trained analysts to do the work. The process of determining the appropriate standard, and then applying that standard to intelligence and law enforcement information that is sometimes wrong, generally incomplete, often conflicting and routinely ambiguous, requires an infrastructure and a well trained, disciplined work force. Quality control is everything. Performing this function in a haphazard fashion, in essence letting a thousand flowers bloom, whereby individuals from any Department or Agency can enter a name on a watchlist, or add information to an existing entry, will result in an unacceptable number of mistakes and reinforce the view that the government is sloppy. And bad guys will routinely slip through the cracks.

Fortunately, the counterterrorism-related investments made by the Country since 9/11 could be readily leveraged in these efforts. We already have the existing TIDE database software which could be replicated for use by those responsible for maintaining the repositories for other categories of bad actors.

Step 2: Focus on Improved Collection and Information Sharing

Maintaining, enhancing, and quality controlling such identities-related databases will require both improved collection and sharing of information associated with these other transnational threats. Here again we will need to learn the lessons from counterterrorism where, after 9/11, the Government recognized the need to break down stovepipes and make far more information available to ensure integration of effort. The sad fact is that we've passed laws, written National Strategies, and drafted implementation documentation to facilitate the sharing of terrorism information, but no such concerted effort exists for many other categories of threat information. The changes that need to occur will have many dimensions, but in particular we will require greater focused collection of relevant biographic and biometrics identifiers and associated derogatory information. And we will require increased reports officers to effect dissemination of relevant information. This will go well beyond traditional intelligence organizations. It will require a true "whole of government" effort involving increased information flow from not only our intelligence collectors, but we also need information from our law enforcement entities – federal and non-federal. System of Records Notices (SORNs) will undoubtedly need updating. And the private sector could be a valuable partner in these efforts. We'll need to broker arrangements with foreign partners to share information in the same way we do for terrorism. Finally, as with any instances when bad actors might come before the U.S. judicial system, we will need to account for pre-trial discovery procedures and the protection of classified information; while the challenges would be significant and must be carefully addressed, that doesn't obviate the need for those responsible for maintaining the databases of transnational nefarious actors to have broad access to relevant information to richly populate those databases.

Step 3: Create a National Watchlisting Center

The Terrorist Screening Center, created by Homeland Security Presidential Directive 6 in 2003, needs to have its charter formally expanded to become a National Watchlisting Center (NWC). At this point it would be authorized to receive the relevant information on all categories of "bad guys" that are being databased by the organizations chartered above to do so. And the NWC would then make such information available to the screening community to assist in encounter management and the decision making process as to whether to grant them visas or allow them into the Country. And importantly, just as is the case with the TSC and potential terrorists, this National Screening Center would have an "operational deconfliction" mission; when we encounter a prospective bad actor we may want to keep him out... or we may want to let him in so that law enforcement can continue an investigation. The terrorist screening center facilitates those conversations when we encounter KSTs and a National Watchlisting Center would enable such coordination across the entire spectrum of potential bad actors. Yet another critical step toward an integrated, whole of government approach to national security.

And the kinds of business processes and technical linkages established for counterterrorism could be used in the creation of such a National Watchlisting Center. We could pattern the watchlisting guidance after the approach used by the CT community - helping enable the rules based, standards based processes to determine who should and who shouldn't be watchlisted (and the nature of that watchlisting). And the technical "handshake" between NCTC and TSC via TIDE/TSDB could be easily replicated by those organizations using the TIDE software to maintain their equivalent database of other categories of bad actors.

Step 4: Utilize these Capabilities to Implement Deeper and Continuous Recurrent Vetting

The Kingfisher program at NCTC has demonstrated the potential for uncovering known and suspected terrorists through large scale data correlation, and this kind of capability could be adopted to help uncover other categories of transnational bad actors. As the data bases of other non-terrorist categories of nefarious actors are maintained, enriched and quality controlled, they will contain a treasure trove of information against which bulk data sets can be continuously compared. An enhanced ability to do entity disambiguation and a greater capacity to process ever increasing amounts of information will enable us to befar more efficient at detecting known or suspected bad guys. The potential for near real time evaluations of visa applicants, as well as the evaluations of those applying for Electronic System of Travel Authorization (ESTA), has already been demonstrated in a counterterrorism context, and now could be extended to all other categories of individuals of national security concern.. For instance, all varieties of Security Advisory Opinions could be vetted in this manner - saving extraordinary amounts of interagency time and money, and expediting legitimate travel. EB-5 investor visa fraud... cyber mules seeking to enter the country to move large amounts of money overseas... money launderers seeking to use our financial system... proliferators looking to acquire dual use technologies... traffickers looking to move people or illicit commodities into the U.S.... transnational criminals looking to conduct medicare fraud... or even spies looking to get access to a security clearance and infiltrate our Intelligence organizations... So long as we have a rich, high quality data base of various categories of nefarious actors, we can utilize the repositories to enhance our collective security. The potential applications would be limited only by our imagination -- in much the same way that bad guys' ability to exploit our openness has only been limited by their imagination.

And as we begin to get ourselves on the same playing field with these exceptionally nimble actors, we'll have an added capability that was developed in the CT context. We will have recurrent vetting always "running in the background", allowing our assessments to be continually updated as new information comes in. No longer will our evaluation be constrained to a particular point in time. Recognizing that we learn immense amounts about new and existing bad guys on a daily basis, we will be addressing the inherent latency challenge posed by out-of-date intelligence. We will be a “learning” organization capable of routinely and continually updating our assessments.

Devilish Details: While the broad contours of the approach and the associated roadmap are laid out in the four steps outlined above, there will be other details that must be addressed:

- Resources: There is no question that there would be upfront resource requirements. As noted above, identities analysis done correctly is a people intensive discipline. But at the same time we don’t need to replicate the entire CT business process. The potential threat of a terrorist attack caused us to fashion a very large enterprise with collectors reviewing their own reporting and then nominating prospective known or suspected terrorists to NCTC; no detail was considered too small. This would not be the case for other threat categories. The organizations responsible for maintaining the all-source databases associated with other transnational actors would build profiles to query incoming intelligence reporting; they would then consolidate relevant information into a TIDE-like data base. We could then leverage the existing counterterrorism IT architecture, thereby limiting the resource requirement. Moreover, our partner organizations might foot parts of the bill, as they have done with Kingfisher.

- Greater Focus on Biometrics. We’ve come a long ways since HSPD-24 was signed in 2008, but biometrics is still in its infancy. And the U.S. is far behind many other Countries. It’s a bit of a “wild west” across the Government and the situation cries out for some order. With the number of repositories, and with different approaches being taken by different Departments and Agencies, we need a concerted effort to lay out a vision that addresses the collection, sharing, processing and use of biometrics. Such an effort must include the closer integration of biographic and biometric identifiers.

- Modernize Names-Based Screening Systems. We’ve still got names-based screening systems that vary widely in sophistication; some utilize advanced “fuzzy” logic, whereas others require exact name matches and may even truncate names after a certain number of characters. There is no question that names-based systems, as a means of establishing identity, are on the wrong side of history; but they are going to be with us for the foreseeable future, and we can do far better than we are now. Government-wide incorporation of “fuzzy” algorithms that account for alternative spellings of common names, and the adoption of standard transliteration protocols, need to be pursued, and automated.

- Streamline Downgrading Procedures for the Purposes of Screening. The terrorism watchlist procedures only work because the government made a collective decision after 9/11 to allow default classification downgrading for those criteria required to support screening. Rather than being required to check with the relevant collector each time a piece of information was required to support the watchlisting system, the screening community was authorized to use particular categories of necessary information (names, passport numbers, pictures, and so forth). However, in particularly sensitive circumstances, the collectors could limit further use of the information. A similar risk-based arrangement that allows broad use of screening information will be required for a viable national watchlist extending beyond that used for counterterrorism purposes.

- Security Challenges. For some categories of bad guys we simply won’t be able to sanitize information and make it broadly available to the screening community. This would be the case for particularly sensitive counterintelligence and economic espionage cases. In these instances the highly classified data base could be used in “Kingfisher-like” capacity so that, for instance, visitors to extremely sensitive research and development facilities could be cross correlated against such a list in order to warn about the prospect of inappropriate visitors. Similarly this approach would lend itself to recurrent vetting of individuals who have security clearances. These particularly sensitive screening imperatives could be accomplished in an entirely classified environment to ensure operational security.

- Further Steps Called For: The Federal Government can start getting serious about tracking significant categories of bad guys, but that will only get us so far. Known transnational criminals have proven able to make use of our financial system because of beneficial ownership provisions that allow total anonymity. For instance, Viktor Bout, a notorious weapons trafficker convicted of conspiring to kill Americans was linked to a dozen shell companies in the United States; he was able to maintain anonymity because of very weak “know your customer” provisions. The Intelligence Community could theoretically do a perfect job identifying transnational bad guys, but unless and until the Country gets serious about beneficial ownership provisions, our financial system will remain vulnerable to exploitation.

- Authorities and a Center Construct: The approach laid out in this paper could probably work under a variety of organizational constructs, but the cleanest would almost certainly occur under a “Center” approach in which form followed function. Empowered in a manner similar to the National Counterterrorism Center, other Centers could focus on proliferation, transnational organized crime, cyber and threat finance. The maintenance of a knowledge base focused on such relevant bad actors would be a natural responsibility for such Centers.

- Evolution of Roles and Responsibilities: As the ability to do large scale “Kingfisher-like” screening across entire categories of bad guys grows, we’ll need to think through the implications for roles and responsibilities. As is the case across the USG, there is a blurring of J2/J3, intelligence/operational responsibilities, and the lash up will be tricky.

IMAGINING THE FUTURE

2nd Order Benefits

These databases will have many other collateral benefits. In the same way that TIDE has enabled us to develop empirical data detailing the extent of the Syrian Foreign Fighter problem, these other databases will support evidence based assessments of other transnational challenges. Current Government claims associated with the scope and scale of such issues as transnational crime and trafficking are often derivative of NGO and academic research that has been shown to be at least questionable. The more rigorous we are in cataloguing data associated with such activities, the more credible our quantitative and qualitative assessments will be.

a. *Getting Ahead of Bad Actors -- other than just Terrorists:* The value of master repositories of known and suspected bad guys is virtually self-evident. Imagine the use the Government could make of what the IRTPA calls, in the terrorist identities context, a “central and shared knowledge bank”. High quality repositories of biographic and biometric identifiers and associated derogatory, enriched with other relevant information could assist other Departments and Agencies in the performance of their statutory missions; for instance, they would be of extraordinary value to the Departments of State (for visas), Homeland Security (for border security), Treasury (for sanctions), Defense (for sensitive facility visits). Commerce (for CFIUS cases) and all Law Enforcement entities (for investigations). We would have, in effect, created a common operating picture of those individuals considered to be threats to our national security. The government would be far better postured to prevent individuals from taking advantage of our openness and lack of government-wide integration.

b. *Using the Intelligence Community Information Technology Environment (ICITE) to Help Integrate U.S. Government-wide Efforts against Transnational Actors:* With standardized "TIDE-like" data bases of various categories of bad actors in the IC cloud, the potential will exist to substantially enhance our ability to do network analysis; structured repositories that could be linked in the Cloud could help uncover previously unknown linkages across separate categories of bad guys. Similarly, ICITE will further enable, and empower, our identities' analysis in support of non IC partners. Imagine an individual pulled into secondary on the U.S. Canadian border - his prints and photo are taken and a cross domain search allows them to be immediately run against the central repository of ALL "bad guy" biometrics in the Intelligence Community cloud; IC elements could then work with the relevant Department or Agency to determine the risk the individual poses to the Country.

c. *Promoting a Global Approach to Collectively Addressing Transnational Problems*: as we're improving our bilateral and multilateral sharing of terrorism information we should be doing the same thing with other transnational bad guys. All elements of state power could be brought together to leverage intelligence and operational capabilities against collective problems. There would be non-trivial privacy issues to be addressed, but we could start with something easy – for instance the global sharing of identities-related information of those who have been convicted of sexual exploitation of minors. We could promote a biometrically enabled global registry of those who have abused minors. Like minded countries could be made aware of such individuals should they be moving internationally. INTERPOL and EUROPOL would be natural partners for appropriate USG Departments and Agencies in such an effort. Eventually this kind of effort could expand and lead to a broader sharing and development of an international watchlist of nefarious transnational actors.

d. *Enhancing our Counterterrorism Posture*: In the same way that transnational criminal actors are rarely single discipline bad guys, history is full of examples of terrorists that were identified as some other flavor of bad guy, long before they were known to be terrorists. Many of the "lone wolves" who weren't known to be associated with ISIS until after their attempted attack would have been inadmissible into the United States on other grounds, such as having been convicted for drug trafficking offenses or other serious crimes. In other words should a convicted trafficker be trying to come to the United States to conduct an attack on our rail system (someone like Ayoub Khazzani who attempted such a plot in France), a robust information sharing regime could have resulted in the individual being watchlisted. Criminal history could have precluded a prospective terrorist from entering the country and conducting an attack - even though he wasn't identified as a known or suspected terrorist at the time.

e. *Beyond Tracking Bad Guys*: As powerful as these tools could be for uncovering and cataloguing "bad guys", appropriate Departments and Agencies could also use them to help assist victims – for instance, those who are being exploited by sex and labor traffickers.

> Imagine a shared photographic repository of family-provided pictures of individuals who have disappeared and are suspected of being subjected to trafficking. Such a watchlist, empowered by ever improving facial recognition tools, could be used globally by border control agents and law enforcement officers who might encounter these vulnerable exploited individuals

CONCLUSIONS

As the Country struggles to deal with the downsides of globalization, the integration challenges are very much whole-of-government in nature; of course we need to continue the process of integrating the Intelligence Community. But 21st century threats require that we think broader. Bringing together relevant lawfully collected information to populate high quality transnational "bad guy" databases, and using that information on behalf of the national security of the Country, ought to be a core function of the Government. Indeed that requirement has already been levied on us in National Strategies such as that issued for Countering Transnational Organized Crime; we were explicitly told to limit TOC actors' ability to travel internationally and enter the Country. Sadly, we have done comparatively little to advance that directive. Unfortunately, in an era of scarce resources, the foundational work of maintaining databases is too often seen as "nice to do". That's a mistake. Cataloguing this kind of tactical information is fundamental to understanding the problem and posturing ourselves to deal with threats that are inherently all about people and networks. We need a strategic framework for dealing with these tactical challenges – individual bad actors that can manifest themselves as true national security threats. Fortunately our counterterror efforts have provided a blueprint for success. We just need to adopt it.